254-45

#3.

Rec'd PCT/PTO 10 MAR 1998

UNITED STATES PATENT AND TRADEMARK OFFICE

08/981882

Applicants: Alcorn et al.
Serial No: 08/981,882
Int'l App. No.: PCT/US96/10463

Atty Docket: 38184-0026US
Filed: December 29, 1998
Filed: June 17, 1996

Title: **"ELECTRONIC CASINO GAMING SYSTEM WITH IMPROVED PLAY CAPACITY, AUTHENTICATION AND SECURITY"**

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

RESPONSE TO NOTICE TO FILE MISSING PARTS

Enclosed herewith for filing in the above-identified application are the following:

1) Copy of Notice Notification of Missing Requirements Under 35 U.S. C. 371 in the United States Designated/Elected Office (DO/EO/US), mailed March 5, 1998;
2) 1 originally executed Verified Statement Claiming Small Entity Status (Small Business Concern);
3) 1 originally executed Declaration and Power of attorney;
4) Check No. 120415 in the amount of $65.00, as payment of the required fees; and
5) Postcard for date-stamped return as confirmation of receipt of these items.

Total fees due in this application amount to $65.00. The Commissioner is further authorized to charge any required additional fees, or credit any overpayment, to deposit account 02-3964.

Respectfully submitted,

Date: March 10, 1998

Claude A.S. Hamrick
Reg. No. 22,586

OPPENHEIMER WOLFF & DONNELLY LLP
Ten Almaden Blvd., Suite 600
San Jose, CA 95113
Tel: (408) 275-8790

I hereby certify that this correspondence with all attachments is being deposited with the U.S. Postal Service as "Express Mail Post Office to Addressee" under 37 CFR 1.10 as Express Mail No. EL059238268US, in an envelope addressed to: BOX PCT, Assistant Commissioner for Patents, Washington, D.C. 20231 on March 10, 1998, by I. Marie Kotsubo.

FORM PTO-1390 (REV 10-96) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 38184-0026US

U S APPLICATION NO (If known, see 37 CFR 1 5): 08/981882

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT /US96/10463	17 June 1996	29 June 1995

TITLE OF INVENTION: Electronic Casino Gaming System with Improved Play Capacity, Authentication and Security

APPLICANT(S) FOR DO/EO/US: ALCORN, Allen E.; BARNETT, Michael; GIACALONE, Louis, D.; LEVINTHAL, Adam E.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U S.C. 371.
3. ☐ This express request to begin national examination procedures (35 U.S.C 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S C 371(b) and PCT Articles 22 and 39(1)
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (Unsigned)
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3 31 is included
13. ☐ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: Filed by Express Mail EM412285650US, on December 29, 1997, by I. Marie Kotsubo.

I Marie Kotsubo

U S APPLICATION NO (if known, see 37 CFR 1 5)	INTERNATIONAL APPLICATION NO PCT/US96/10463	ATTORNEY'S DOCKET NUMBER 38184-0026US

17. [X] The following fees are submitted:

		CALCULATIONS PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Search Report has been prepared by the EPO or JPO	$910.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482)	$700.00	
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))	$770.00	
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$1040.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	$98.00 ~~$1000~~	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$ 98.00
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).		$

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE	
Total claims	62	- 20 =	42	X $22.00 ~~82.00~~	$ 924.00
Independent claims	9	- 3 =	6	X $80.00 ~~$82.00~~	$ 492.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ $260.00	$
TOTAL OF ABOVE CALCULATIONS =					$ 1,514.00
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).					$
SUBTOTAL =					$ 1,514.00
Processing fee of **$130.00** for [illegible] English translation later than [ ] 20 [ ] 30 months from the earliest claimed [illegible] (37 CFR 1.492(f)) +					$
TOTAL NATIONAL FEE =					$
Fee for recording the enclosed assignment (37 CFR 3.28, 3.31) **$40.00** per property + The assignment must be accompanied by an appropriate cover sheet					$
TOTAL FEES ENCLOSED =					$1,514.00
				Amount to be: refunded	$
				charged	$

a. [X] A check in the amount of $ 1,514.00 to cover the above fees is enclosed. Check No. 120280

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No 02-3964. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO
Claude A.S. Hamrick, Reg. No.# 22,586
OPPENHEIMER POMS SMITH
Ten Almaden Boulevard, Suite 600
San Jose, California 95113
United States of America
PH. (408) 275-8790
FAX (408) 275-8793

SIGNATURE

NAME Maryam Imam

38,190
REGISTRATION NUMBER

Specification

ELECTRONIC CASINO GAMING SYSTEM WITH IMPROVED PLAY CAPACITY, AUTHENTICATION AND SECURITY

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to microprocessor based gaming Systems used in gambling casinos.

Brief Description of the Prior Art

Microprocessor based gaming systems are known which are used in gambling casinos to augment the traditional slot machine games (e.g. three reel single or multi-line games) and card games, such as poker and black jack. In a typical gaming system of this type, a microprocessor based system includes both hardware and software components to provide the game playing capabilities. The hardware components include a video display for displaying the game play, mechanical switches for enabling player selection of additional cards or game play choices, coin acceptors and detectors and the electronic components usually found in a microprocessor based system, such as random access memory (RAM), read only memory (ROM), a processor and one or more busses. The software components include the initialization software, credit and payout routines, the game image and rules data set, and a random number generator algorithm. In order to be acceptable for casino use, an electronic gaming system must provide both security and authentication for the software components. For this reason, gaming commissions have heretofore required that all software components of an electronic gaming system be stored in unalterable memory, which is typically an unalterable ROM. In addition, a copy of the contents of the ROM or a message digest of the contents (or both) are normally kept on file in a secure location designated by the gaming commission so that the contents of an individual ROM removed from a gaming machine can be verified against the custodial version.

In a typical arrangement, a message digest of the ROM contents is initially generated prior to the installation of the ROM in the machine by using a known

algorithm usually referred to as a hash function. A hash function is a computation procedure that produces a fixed-size string of bits from a variable-size digital input. The fixed-sized string of bits is termed the hash value. If the hash function is difficult to invert -- termed a one-way hash function -- the hash function is also termed a message digest function, and the result is termed the message digest. The message digest is unique to any given variable size input data set, i.e., the game data set stored in the ROM. When it becomes necessary to later authenticate the ROM from any given machine, the ROM is physically removed from the game console and the message digest of the ROM contents is computed directly from the ROM using the original hash function. The computed message digest is compared with the message digest on file at the designated custodial location (typically in the casino itself). This procedure is typically carried out whenever a machine produces a payoff beyond a given threshold value. If the two message digests match, then the contents of the ROM are considered to be authenticated (verified) and the payout is made to the player.

While such electronic casino gaming systems have been found to be useful in promoting casino game play, the restriction requiring that the casino game program be stored in unalterable ROM memory, leads to a number of disadvantageous limitations. First, due to the limited capacity of the ROM storage media traditionally used to hold the program, the scope of game play available with such systems is severely limited. For sophisticated games using motion video and audio multi-media elements, much more memory capacity, on the order of hundreds of megabytes, is necessary. However, physical verification of such a large quantity of physical devices is not practical, and has thus far been an impediment to creating sophisticated games with more player appeal. Second, the authentication check is only conducted on a limited basis (usually after a jackpot) or other significant winning game outcome, and the authentication procedure requires that game play be halted until the ROM contents have been found to be authentic.

SUMMARY OF THE INVENTION

The invention comprises an electronic casino gaming system which greatly expands casino game play capability and enhances security and authentication capabilities. More particularly, the invention comprises an electronic casino gaming

system and method having greatly expanded mass storage capability for storing a multiplicity of high resolution, high sound quality casino type games, and provides enhanced authentication of the stored game program information with a high security factor.

According to a first aspect of the invention, authentication of a casino game data set is carried out within the casino game console using an authentication program stored in an unalterable ROM physically located within the casino game console. The casino game data set and a unique signature are stored in a mass storage device, which may comprise a read only unit or a read/write unit and which may be physically located either within the casino game console or remotely located and linked to the casino game console over a suitable network. The authentication program stored in the unalterable ROM performs an authentication check on the casino game data set at appropriate times, such as prior to commencement of game play, at periodic intervals or upon demand. At appropriate occasions, the contents of the unalterable ROM can be verified by computing the message digest of the unalterable ROM contents and comparing this computed message digest with a securely stored copy of the message digest computed from the ROM contents prior to installation in the casino game console.

From a process standpoint, this aspect of the invention comprises a method of authenticating a data set of a casino style game which consists of two phases: a game data set preparation phase and a game data set checking phase. In the game data set preparation phase, the method proceeds by providing a data set for a casino game, computing a first abbreviated bit string unique to the casino game data set, encrypting the first abbreviated bit string to provide an encrypted signature of the casino game data set, and storing the casino game data set and the signature in a mass storage device. The first abbreviated bit string is preferably computed using a hash function to produce a message digest of the casino game data set. The signature is then encrypted from the message digest. After storage of the game data set and unique signature, this information is installed in a casino game console. The casino game data set checking phase proceeds by computing a second abbreviated bit string from the stored casino game data set using the same hash function, decrypting the stored encrypted signature to recover the first abbreviated bit string, and comparing the first and second abbreviated bit strings to determine whether the two strings

match. If a match does occur, the casino game data set is deemed authentic; if there is no match, authentication is denied and game play is prohibited.

The encryption/decryption process is preferably performed using a private key/public key technique in which the first abbreviated bit string is encrypted by the game manufacturer using a private encryption key maintained in the custody of the game manufacturer. The decryption of the signature is performed using a public key which is contained in an unalterable read only memory element located in the game console, along with the casino game data set. The casino game data set is preferably stored in a mass storage device, such as a magnetic or CD-ROM disk drive unit or a network file unit, the selected unit having a relatively large capacity. The actual size of the mass storage device will depend upon the casino game storage requirements and can be tailored to any specific application.

Each time a casino game data set is transferred from the mass storage device to the main memory of the system, the authentication routine is run. The authentication routine can also be means of an operator switch mounted in the game console or remotely via a network. Consequently, the authenticity of the data set can be automatically checked whenever the transfer occurs and at other appropriate times.

In order to detect attempts to tamper with the contents of the unalterable read only memory element located in the game console, a message digest computed for the authentication program stored therein is stored in a secure manner in a different location from the game console, such as the casino operator's security facilities or the facilities of a gaming commission (or both). The authenticity of the unalterable read only memory element is checked in the same way as that now performed in prior art devices: viz. computing the message digest directly from the unalterable read only memory device, and comparing the message digest thus computed with the custodial version.

From an apparatus standpoint, the first aspect of the invention comprises an electronic casino gaming system having means for providing authentication of a game data set of a casino type game prior to permitting game play, the system including first means for storing a casino game data set and a signature of the casino game data set, the signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game data set; second means for storing an authentication program capable of computing a second abbreviated bit

string from the casino game data set stored in the first storing means and capable of decrypting the encrypted signature stored in the first storing means to recover the first abbreviated bit string; processing means for enabling the authentication program to compute an abbreviated bit string from the casino game data set stored in the first storing means and for enabling the authentication program to decrypt the encrypted signature; and means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present. The first storing means preferably comprises a mass storage device, such as a disk drive unit, a CD-ROM unit or a network storage unit. The second storing means preferably comprises an unalterable read only memory in which the authentication program is stored.

According to a second aspect of the invention, the authentication program stored in the unalterable ROM located within the casino game console is used to test the authenticity of all other programs and fixed data stored in memory devices in the electronic casino gaming system, such as a system boot ROM, memory devices containing the operating system program, system drivers and executive/loader programs, and other memory devices incorporated into the electronic casino game system architecture. The contents of each such memory device, whether program information or fixed data, include signatures encrypted from message digests computed using a hash function from the original program information or fixed data set. Upon system initialization, the authentication program in the unalterable ROM is used to authenticate the individual memory device contents in essentially the same fashion as that used to authenticate the casino game data sets. More specifically, the message digest for the given program or fixed data set is computed using the same hash function originally used to produce the message digest for that program or fixed data set. The encrypted signature is decrypted using the proper decryption program and decryption key to recover the message digest. The two versions of the message digest are then compared and, if found to be matching, the concerned program or fixed data set is deemed authentic and is permitted to be used by the system. Once all of the concerned programs and fixed data sets have been so authenticated. the casino game data set authentication procedure is run, after which game play is permitted (provided a match occurs).

From a process standpoint, this second aspect of the invention comprises a method of authenticating a program or data set of a casino style game which consists of two phases: a program or fixed data set preparation phase, and a program or fixed data set checking phase. In the program or fixed data set preparation phase, the method proceeds by providing a program or fixed data set for a casino game, computing a first abbreviated bit string unique to the program or fixed data set, encrypting the first abbreviated bit string to provide an encrypted signature of the program or fixed data set, and storing the program or fixed data set and the signature in a memory device. The first abbreviated bit string is preferably computed using a hash function to produce a message digest of the program or fixed data set. The signature is then encrypted from the message digest. After storage of the program or fixed data set and unique signature in the memory device, the memory device is installed in a casino game console. The casino game program or fixed data set checking phase proceeds by computing a second abbreviated bit string from the stored casino game program or fixed data set stored in the memory device using the same hash function, decrypting the encrypted signature stored in the memory device to recover the first abbreviated bit string, and comparing the first and second abbreviated bit strings to determine whether the two strings match. If a match does occur, the casino game program or fixed data set is deemed authentic; if there is no match, authentication is denied and use of that casino game program or fixed data set is prohibited.

The authentication routine is run each time a given casino game program or fixed data set needs to be called or used. The authentication routine can also be run automatically on a periodic basis, or on demand -- either locally by means of an operator switch mounted in the casino game console or remotely via a network. Consequently, the authenticity of the casino game program or fixed data set can be automatically checked whenever use of that program or fixed data set is required and at other appropriate times, such as in the course of a gaming commission audit.

From an apparatus standpoint, this second aspect of the invention comprises an electronic casino gaming system for providing authentication of a casino game program or fixed data set prior to permitting system use of that casino game program or fixed data set, the system including first means for storing a casino game program or fixed data set and a signature of the casino game program or fixed data set; the

signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game program or fixed data set; second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game program or fixed data set stored in the first storing means and capable of decrypting the encrypted signature stored in the first storing means to recover the first abbreviated bit string; processing means for enabling the authentication program to compute an abbreviated bit string from the casino game program or fixed data set stored in the first storing means and for enabling the authentication program to decrypt the encrypted signature; and means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present. The first storing means preferably comprises a memory device, such as a read only memory or random access memory. The second storing means preferably comprises an unalterable read only memory in which the authentication program is stored.

Electronic casino game systems incorporating the invention provide a vastly expanded capacity for more sophisticated and attractive casino-style games, while at the same time improving the authentication of the games without compromising security. In addition, casino game systems incorporating the invention provide great flexibility in changing casino game play, since the casino game data sets representing the various games can be stored in alterable media rather than read only memory units as with present casino game systems.

By separating the authentication process from the casino game data set storage, the invention affords secure distribution and execution of program code and data, regardless of the particular distribution or storage technique employed. More specifically, the invention allows the casino game data set to reside in any form of secondary storage media, such as the traditional ROM storage, hard magnetic disk drives and CD-ROM drives, or networked file systems. So long as the authentication procedure conducted on the game data set is performed using the authentication program stored in an unalterable ROM, and so long as that ROM can be verified reliably, any casino game data set can be loaded from any source and can be verified by the system at any time: either prior to use, during run-time, periodically during run-time or upon demand. The large quantities of storage that can be made available in a secure fashion using the invention, facilitates the creation of casino gaming

systems offering both an increased diversity of games, and individual games of superior quality. In addition, the authentication of all casino game program and fixed data software ensures the integrity of all system software both prior to game play and thereafter at periodic or random intervals.

For a fuller understanding of the nature and advantages of the invention, reference should be had to the ensuing detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a system incorporating the invention;

FIG. 2 is a schematic diagram illustrating the contents of the read only memory and the mass storage device;

FIG. 3 is a more detailed schematic view of the authentication program stored in the ROM and the game data stored in the mass storage unit;

FIG. 4 is a diagram illustrating the preparation of the game data set;

FIG. 5 is a diagram illustrating the authentication procedure for the game data set; and

FIG. 6 is a diagram illustrating an alternative approach to the secure loading of software into the system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning now to the drawings, FIG. 1 is a block diagram of an electronic casino gaming system incorporating the invention. As seen in this figure, the system consists of several system components under software control. These system components include a microprocessor 12, which may comprise any general purpose microprocessor, such as a Pentium-based microprocessor from Intel Corporation. A main memory unit 13 is provided, which is typically a random access memory having a capacity of between 32 and 64 megabytes for storing the majority of programs and graphics elements during game play. A system boot ROM 14 provides the initialization software required when power is first applied to the system. ROM 14 contains additional programs in read only form, including the operating system, related drivers and the authentication software described in detail below. A non-volatile RAM 17 is a battery backed static RAM capable of maintaining its contents

through power cycling. NV RAM 17 stores significant information relating to game play, such as the number of player credits, the last game outcome and certain diagnostic and error information not critical to an understanding of the invention.

A mass storage unit implemented in the Fig. 1 system as a magnetic hard disk drive unit 18 is coupled to and controlled by a disk subsystem 19 of conventional design and operation. Disk drive unit 18 provides storage for the game specific data set, which includes both program data and image data specifying the rules of the various different casino games or single casino game variations, and the types of images and image sequences to be displayed to the game players. The size of the disk drive unit 18 is a function of the number of games and game variations provided for a given system, as well as the amount of data required for each specific game. In general, the more motion video designed into a particular casino game, the more storage required for that casino game software. A disk drive unit 18 with a 4-gigabyte capacity will usually provide sufficient storage capacity. Disk subsystem 19 comprises a disk controller connected to a PCI bus 20 for controlling the disk drive unit 18. Controller 19 preferably supports SCSI-2, with options of fast and wide. It should be noted that a number of different types of locally-based disk drive units may be used in the Fig. 1 system, including a CD-ROM storage unit. Also, the mass storage unit need not be physically located within the game console along with the other elements depicted in Fig. 1: the mass storage unit may be located remotely from the game console and coupled thereto by means of an appropriate network, such as an ethernet, an R5232 link, or some other hard-wired or wireless network link. This latter alternate arrangement is indicated by the inclusion of a network subsystem 21 of appropriate configuration and functional characteristics, which may have ethernet, R5232 serial, or other network compatibility.

A video subsystem 22 is coupled to the PCI bus and provides the capability of displaying full color still images and MPEG movies with a relatively high frame rate (e.g. 30 frames per second) on an appropriate monitor (not shown). Optional 3D texture mapping may be added to this system, if desired.

A sound subsystem 23 having a stereo sound playback capability with up to 16 bit CD quality sound is coupled to an ISA bus 24. A general purpose input/output unit 25 provides interfaces to the game mechanical devices (not illustrated) such as manually actuatable switches and display lights. A first bridge

circuit 27 provides an interface between microprocessor 12, ROM 14, main memory 13 and PCI bus 20. Bridge circuit 27 is preferably a TRITON chip set available from INTEL Corporation. A second bridge circuit 28 provides an interface between the PCI bus 20 and the ISA bus 24. Bridge circuit 28 is preferably a type 82378 chip available from Intel Corporation.

Fig. 2 illustrates the types of information stored in the system ROM 14 and the mass storage unit. As seen in Fig. 2, the ROM unit 14 used in the Fig. 1 system comprises two separate ROM elements: ROM 29 and ROM 30. ROM 29 must be an unalterable device, such as a Toshiba type C53400 512Kx8 bit mask programmed ROM. ROM 30 is preferably an unalterable device like ROM 29, but may comprise a different type of ROM, such as a type 29FO40 field programmable flash ROM available from Intel Corp. ROM 29 contains the system initialization or boot code, an authentication program, a random number generator program and an initial portion of the executive/loader programs. ROM 30 contains the operating system program, the system drivers and the remainder of the executive/loader programs as noted below. The mass storage unit contains the applications, which include the game image and sound data, rules of game play and the like, and the signature associated to each particular casino game.

Fig. 3 illustrates the authentication and application program information in more detail. As seen in this figure, the authentication program stored in unalterable ROM 29 comprises a message digest algorithm component 32, a decryption algorithm component 33, and a decryption key component 34. The message digest algorithm component 32 stored in ROM 29 comprises an exact copy of a hash function program routine used to originally compute a message digest from the loadable game data set 36 in the manner described below. The decryption algorithm component 33 stored in ROM 29 comprises the algorithm required to decrypt any encrypted casino game data set signature using the decryption key component 34.

The decryption key component 34 comprises the decryption key that is required to decrypt any of the encrypted signatures 37 in the manner described below during the authentication routine.

Fig. 4 illustrates the manner in which an encrypted data set signature 37 is generated. A loadable casino game data set 36 is processed using a hash function 41 to generate a message digest 42 which is unique to the loadable game data set 36.

The hash function employed may be one of a number of known hash functions, such as the MD2, MD4, and MD5 hash functions and the SHS hash function; or any other suitable hash function capable of producing a unique abbreviated bit string from a variable size input data set. For further information about these hash functions, reference should be had to the publication entitled "Answers To Frequently Asked Questions About Today's Cryptography", Revision 2.0, October 5, 1993, published by RSA Laboratories, Redwood City, California, and the publications listed in the references section thereof, the disclosures of which are hereby incorporated by reference. After generation, the message digest 42 is then encrypted with an encryption algorithm 43 using a private encryption key 44 to generate a signature 37 of the message digest. In the preferred embodiment, the two-key (private/public key) encryption technique developed by RSA Data Security, Inc., of Redwood City, California, is used. This technique is disclosed and described in U.S. Patent Nos. 4,200,770, 4.218,582 and 4,405,829, the disclosures of which are hereby incorporated by reference. The signature 37 of the message digest 42 is then stored in the mass storage unit along with the loadable data set 36.

Fig. 5 illustrates the authentication routine carried out in accordance with the invention. when the authentication routine is called (see below), the loadable casino game data set 36 is transferred from the mass storage unit to main memory 13 (unless already there), and the message digest of casino game data set 36 is computed using the message digest algorithm 32. Message digest algorithm 32 uses the same hash function 41 as that used by the manufacturer to prepare the original message digest 42. The result is an unencrypted version 46 of the message digest computed from the casino game data set 36 currently present in the mass storage unit. The encrypted data set signature 37 is decrypted using the public decryption key 34 matching the private key 44 used to originally encrypt the message digest 42 of the casino game data set 36. The message digest 47 decrypted with decryption key 34 is then compared with the message digest 46 computed from the casino game data set 36. If the two message digests match, then the casino game data set 36 is deemed authentic and game play may proceed. If there is no match, either the casino game data set 36 or the signature 37 is deemed corrupted and not authentic. Game play is prohibited and appropriate actions can be taken: e.g. alerting a security employee

using a suitable messaging system (an audible alarm, flashing lights, or a network message from the game console to a central security area).

In order to ensure that the authentication routine cannot be bypassed by tampering with the loader program stored in ROM 30, an initial part of the loader program is incorporated into unalterable ROM 29. This initial portion of the loader program requires that the authentication program be called prior to the initiation of any casino game play. Since this initial portion of the loader program is located in the unalterable ROM 29, and since no casino game play can occur until the particular casino game application data set 36 is loaded into main memory 13, the authentication procedure cannot be bypassed by tampering with the software stored in ROM 30.

Since authentication of the game data set 36 and signature 37 is entrusted to the contents of ROM 29, a procedure must be provided to verify the ROM 29 contents. For this purpose, a message digest is computed for the authentication program stored in ROM 29, and this message digest is stored in a secure manner with the casino operator or the gaming commission (or both) along with the hash function used to produce the message digest. This hash function may be the same hash function used to compute the message digest 42 of the casino game data set or a different hash function. In this way, the authenticity of the ROM 29 can be easily checked in the same way as that now performed in prior art devices: viz. computing the message digest directly from the ROM 29 and comparing the message digest thus computed with the custodial version of the message digest. If required by a given gaming commission or deemed desirable by a casino operator, the system may also display the message digest 42 of each particular data set 36 or the encrypted signature version 37 for auditing purposes. In addition, the system may transmit this information via networking subsystem 21 to an on-site or off-site remote location (such as the office of the gaming commission). The message digest displayed or transmitted may comprise the decrypted version or the computed version (or both).

The authentication procedure carried out by means of the message digest program 32, decryption program 33 and decryption key 34 stored in unalterable ROM 29 in the manner described above is also used to authenticate the contents of all memory devices in the Fig. 1 system, such as the contents of ROM 30 (see Fig. 2), the fixed data portions and program components stored in NV RAM 17 and the

program and fixed data contents of any memory devices stored in the networking subsystem 21, video subsystem 22, sound subsystem 23, PCI-ISA interface 24, and GPIO unit *25*. Each program or fixed data set stored in any memory device in any of these units has an associated signature, which is encrypted from a message digest of the original program or fixed data set using a hash function, which is preferably the same hash function used to prepare the message digest of the casino game data set. Prior to permitting any such program or fixed data set to participate in the system operation, that program or fixed data set is subjected to the authorization procedure to ensure that the message digest computed from the current version of the program or fixed data set matches the message digest decrypted from the encrypted signature associated to the program or fixed data set. In addition, the authentication procedure can be run on each such program or fixed data set at periodic or random intervals (on demand) in a manner essentially identical to that described above with respect to the casino game data set authentication procedure. As a consequence, the integrity of all software in the system is checked prior to the use of that particular software in order to reveal any unauthorized changes to the software portion of the casino gaming system.

An alternative approach to the secure loading of software into the system is depicted in FIG. 6. In this embodiment the basic input/output system (BIOS) software is stored in a ROM 50, the first of two ROMs making up the system boot ROM 14 (FIG. 1). The boot strap code, operating system code (OS), OS drivers and a secure loader are stored in a second ROM 52. An anchor application 54 including graphics and sound drivers, system drivers, money-handling software, a second secure loader, and a signature is stored in the mass storage 18 (FIG. 1).

When power is initially applied to the system on start-up, or when the system experiences a warm restart, the CPU 12 will begin executing code from the BIOS ROM 50. The BIOS is responsible for initializing the motherboard and peripheral cards of the system. After the BIOS has completed the initialization, it jumps to the boot strap code in ROM 252 causing the boot strap to copy the OS, OS drivers, and the secure loader into RAM.

Once in RAM, the OS is started and the secure loader stored in ROM 52 is used to load the anchor application 54 from disk 18. On disk. the anchor application

has a signature that is used during the load to verify the validity of the anchor application.

After the anchor application 54 is started, it will be used to load all other applications. The secure loader of the anchor application will check the validity of an application to be loaded by computing the signature and comparing it against the one stored on disk with the application as described above.

An important advantage of the invention not found in 20 prior art systems is the manner in which the casino game data set can be authenticated. In prior art systems, authentication of the casino game data set is normally only done when a payout lying above a given threshold is required by the outcome of the game play, and this requires that the game be disabled while the ROM is physically removed and the ROM contents are verified. In systems incorporating the invention, the authenticity of a given casino game data set can be checked in a variety of ways. For example, the game data set 36 can be automatically subjected to the authentication procedure illustrated in Fig. 5 each time the game is loaded from the mass storage unit into the main memory 13. Thus, as a player selects a casino game for game play in the system, the authenticity of that game actually stored in the mass storage unit is automatically checked using the authentication procedure described above without removing the ROM 29. Further, if desired, the authentication procedure may be initiated in response to the pull of a slot game handle, the detection of a coin insert. the payout of coins or issuing of credit, or any other detectable event related to game play. The authenticity of a given casino game data set 36 can also be checked on demand, either locally at the game console or remotely via a network, by providing a demand procedure. Such a procedure may be initiated, e.g. by providing a manually operable switch in the game console, accessible only to authorized persons. for initiating the authentication routine. Alternatively, the Fig. 1 system may be configured to respond to a demand command generated remotely (e.g. in a security area in the casino or off-site) and transmitted to the game console over a network to the networking subsystem 21.

Another advantage of the invention lies in the fact that the game data set storage capacity of a system incorporating the invention is not limited by the size of a ROM, but is rather dictated by the size of the mass storage unit. As a consequence. games using high resolution, high motion video and high quality stereo sound can

be designed and played on systems incorporating the invention. Also, since the mass storage unit need not be a read-only device, and need not be physically located in the game console, the invention affords great flexibility in game content, scheduling and changes. For example, to change the graphic images in a particular casino game or set of games, new casino game data sets can be generated along with new signatures and stored in the mass storage unit by either exchanging disk drives, replacing disks (for read only disk units), or writing new data to the media. In the networked mass storage application, these changes can be made to the files controlled by the network file server. Since the casino game data sets must pass the authentication procedure test, either periodically or on demand, corrupted data sets cannot go undetected. Thus the invention opens up the field of electronic casino gaming systems to readily modifiable games with flexible displays and rules, without sacrificing the essential security of such systems. In fact, security is greatly enhanced by the ability of the invention to authenticate all game data sets both regularly (for each handle pull) and at any time (on demand), without interfering with regular game play (unless no match occurs between the two forms of message digest).

While the above provides a full and complete disclosure of the preferred embodiments of the invention, various modifications, alternate constructions and equivalents may be employed without departing from the true spirit and scope of the invention. For example, while the RSA public/private key encryption technique is preferred (due to the known advantages of this technique), a single, private key encryption technique may be employed, if desired. In a system using this technique, the single key would be stored in ROM 29 in place of the public key 34. Also, the message digest 42 and signature 37 for a given application 36 need not be computed from the entire casino game data set. For example, for some casino games it may be desirable to provide a fixed set of rules while permitting future changes in the casino game graphics, sound or both. For such casino games, it may be sufficient to compute the message digest 42 and signature 37 from only the rules portion of the applications program 36. In other cases, it may be desirable or convenient to maintain the casino game video and audio portions constant, while allowing future changes to the rules of game play. For casino games of this category, the message digest 42 and signature 37 may be computed from the graphics and sound portions of the application program 36. It may also be desirable to compute a message digest

42 and signature 37 from a subset of the rules, graphics or sound portions of a given applications program 36, or from some other subset taken from a given applications program 36. Therefore, the above should not be construed as limiting the scope of the invention, which is defined by the appended claims.

CLAIMS

1. A method of authenticating a data set of a casino-type viewable game, said method comprising the steps of:

(a) providing a data set for a casino game;

(b) computing a first abbreviated bit string unique to the data set;

(c) encrypting the abbreviated bit string to provide a signature;

(d) storing the data set and the signature;

(e) computing a second abbreviated bit string from the stored data set;

(f) decrypting the stored signature to recover the first abbreviated bit string; and

(g) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

2. The method of claim 1 wherein said step (b) of computing is performed with a hash function to produce a hash value of the date set, and wherein said first abbreviated bit string comprises the hash value of the data set.

3. The method of claim 2 wherein the hash value comprises the message digest of the data set.

4. The method of claim 1 wherein said step (c) of encrypting is performed using a private encryption key.

5. The method of claim 1 wherein said step (f) of decrypting is performed using a public decryption key.

6. The method of claim 1 wherein said step (c) of encrypting is performed using a private encryption key, and said step (f) of decrypting is performed using a public decryption key.

7. The method of claim 1 wherein said step (e) of computing is performed with a hash function to produce a hash value of the stored data set, and wherein said second abbreviated bit string comprises the hash value of the stored data set.

8. The method of claim 7 wherein the hash value comprises the message digest of the stored data set.

9. The method of claim 1 wherein said step (d) of storing includes the step of storing the data set and the signature in a mass storage device.

10. The method of claim 9 wherein the mass storage device comprises a disk drive unit.

11. The method of claim 9 wherein the mass storage device comprises a CD-ROM unit.

12. The method of claim 9 wherein the mass storage a network storage system.

13. The method of claim 1 wherein said steps (a)-(d) a first site, and wherein steps (e)-(g) are performed at a second site.

14. The method of claim 13 wherein the first site comprises a manufacturing facility, and wherein said second site is a gaming facility.

15. A method of preparing a casino game data set capable of authentication. said method comprising the steps of:

(a) providing a data set for a casino game;

(b) computing a first abbreviated bit string unique to the casino game data set;

(c) encrypting the abbreviated bit string to provide a signature; and

(d) storing the casino game data set and the signature.

16. The method of claim 15 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game data set, and wherein said first abbreviated bit string comprises the hash value of the stored casino game data set.

17. The method of claim 16 wherein the hash value comprises the message digest of the casino game data set.

18. The method of claim 15 wherein said step (c) of encrypting is performed using a private encryption key.

19. The method of claim 15 wherein said step (d) of step of storing the casino game data set and the signature in a mass storage device.

20. The method of claim 19 wherein the mass storage device comprises a disk drive unit.

21. The method of claim 19 wherein the mass storage device comprises a CD-ROM unit.

22. The method of claim 19 wherein the mass storage device comprises a network storage system.

23. A method of authenticating a casino game data set of a casino type viewable game having a signature encrypted from a first abbreviated bit string computed from the casino game data set, said method comprising the steps of:

(a) computing a second abbreviated bit string from the casino game data set;

(b) decrypting the signature to recover the first abbreviated bit string; and

(c) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

24. The method of claim 23 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game data set, and wherein said second abbreviated bit string comprises the hash value of the casino game data set.

25. The method of claim 24 wherein the hash value comprises the message digest of the casino game data set.

26. The method of claim 23 wherein said step (b) of decrypting is performed using a public decryption key.

27. An electronic gaming system for providing authentication of a data set of a casino type game, said system comprising:

first means for storing a casino game data set and a signature of said casino game data set, said signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game data set;

second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game data set stored in said first storing means and capable of decrypting an encrypted signature stored in said first storing means to recover the first abbreviated bit string;

processing means for enabling the authentication program to compute an abbreviated bit string from the casino game data set stored in said first storing means and for enabling the authentication program to decrypt the encrypted signature stored in said first storing means to provide a decrypted abbreviated bit string; and

means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present.

28. The system of claim 27 wherein said first storing means comprises a mass storage device.

29. The system of claim 28 wherein said mass storage device comprises a disk drive unit.

30. The system of claim 28 wherein said mass storage device comprises a CD-ROM unit.

31. The method of claim 28 wherein said mass storage device comprises a network storage unit.

32. The system of claim 27 wherein said second storing means comprises a read only memory device.

33. The system of claim 32 wherein said read only memory device comprises an unalterable memory device.

34. The system of claim 32 wherein said read only memory device includes a first portion for storing that portion of said authentication program capable of computing the abbreviated bit string from the casino game data set, and a second portion for storing that part of the authentication program capable of decrypting the encrypted signature.

35. The system of claim 34 wherein said second ROM portion is used to store a decryption key.

36. For use in authenticating a casino game data set and signature encrypted from an original message digest computed from the casino game data set; an unalterable read only memory device having stored therein a message digest computing program corresponding to the message digest program used to compute the original message digest of the casino game data set, and a decryption program and decryption key corresponding to the encryption program and encryption key used to prepare the encrypted signature of the original message digest.

37. The device of claim 36 wherein the message digest computing program comprises a hash function.

38. The device of claim 36 wherein the stored decryption key comprises a public key.

39. The device of claim 36 further including an initial loader program stored in said unalterable read only memory device for ensuring use of the message digest computing program, the decryption program and the decryption key.

40. A method of preparing casino game software information capable of authentication, said method comprising the steps of:

(a) providing software information relating to a casino game;

(b) computing a first abbreviated bit string unique to the casino game software information;

(c) encrypting the abbreviated bit string to provide a signature; and

(d) storing the casino game software information and the signature.

41. The method of claim 40 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game software information, and wherein said first abbreviated bit string comprises the hash value of the stored casino game software information.

42. The method of claim 41 wherein the hash value comprises the message digest of the casino game software information.

43. The method of claim 40 wherein said step (c) of encrypting is performed using a private encryption key.

44. The method of claim 40 wherein said step (d) of storing includes the step of storing the casino game software information and the signature in a memory device.

45. A method of authenticating casino game software information having a signature encrypted from a first abbreviated bit string computed from the casino game software information. said method comprising the steps of:

(a) computing a second abbreviated bit string from the casino game software information;

(b) decrypting the signature to recover the first abbreviated bit string; and

(c) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

46. The method of claim 45 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game software information, and wherein said second abbreviated bit string comprises the hash value of the casino game software information.

47. The method of claim 46 wherein the hash value comprises the message digest of the casino game software information.

48. The method of claim 45 wherein said step (b) of decrypting is performed using a public decryption key.

49. An electronic gaming system for providing authentication of software information relating to a casino type game, said system comprising:

first means for storing casino game software information and a signature of said casino game software information, said signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game software information;

second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game software information stored in said first storing means and capable of decrypting an encrypted signature stored in said first storing means to recover the first abbreviated bit string;

processing means for enabling the authentication program to compute an abbreviated bit string from the casino game software information stored in said first storing means and for enabling the authentication program to decrypt the encrypted signature stored in said first storing means to provide a decrypted abbreviated bit string; and

means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present.

50. The system of claim 49 wherein said first storing means comprises a memory device.

51. The system of claim 50 wherein said memory device comprises a read only memory.

52. The system of claim 50 wherein said memory device comprises a RAM.

53. The system of claim 49 wherein said second storing means comprises a read only memory device.

54. The system of claim 53 wherein said read only memory device comprises an unalterable memory device.

55. The system of claim 53 wherein said read only memory device includes a first portion for storing that portion of said authentication program capable of computing the abbreviated bit string from the casino game software information, and a second portion for storing that part of the authentication program capable of decrypting the encrypted signature.

56. The system of claim 53 wherein said second ROM portion is used to store a decryption key.

57. The system of claim 49 wherein said casino game software information comprises program information.

58. The system of claim 49 wherein said casino game software information comprises a fixed data set.

59. For use in authenticating casino game software information and a signature encrypted from an original message digest computed from the casino game software information; an unalterable read only memory device having stored therein a message digest computing program corresponding to the message digest program used to compute the original message digest of the casino game software information, and a decryption program and decryption key corresponding to the encryption program and encryption key used to prepare the encrypted signature of the original message digest.

60. The device of claim 59 wherein the message digest computing program comprises a hash function.

61. The device of claim 59 wherein the stored decryption key comprises a public key.

62. The device of claim 59 further including an initial loader program stored in said unalterable read only memory device for ensuring use of the message digest computing program, the decryption program and the decryption key.

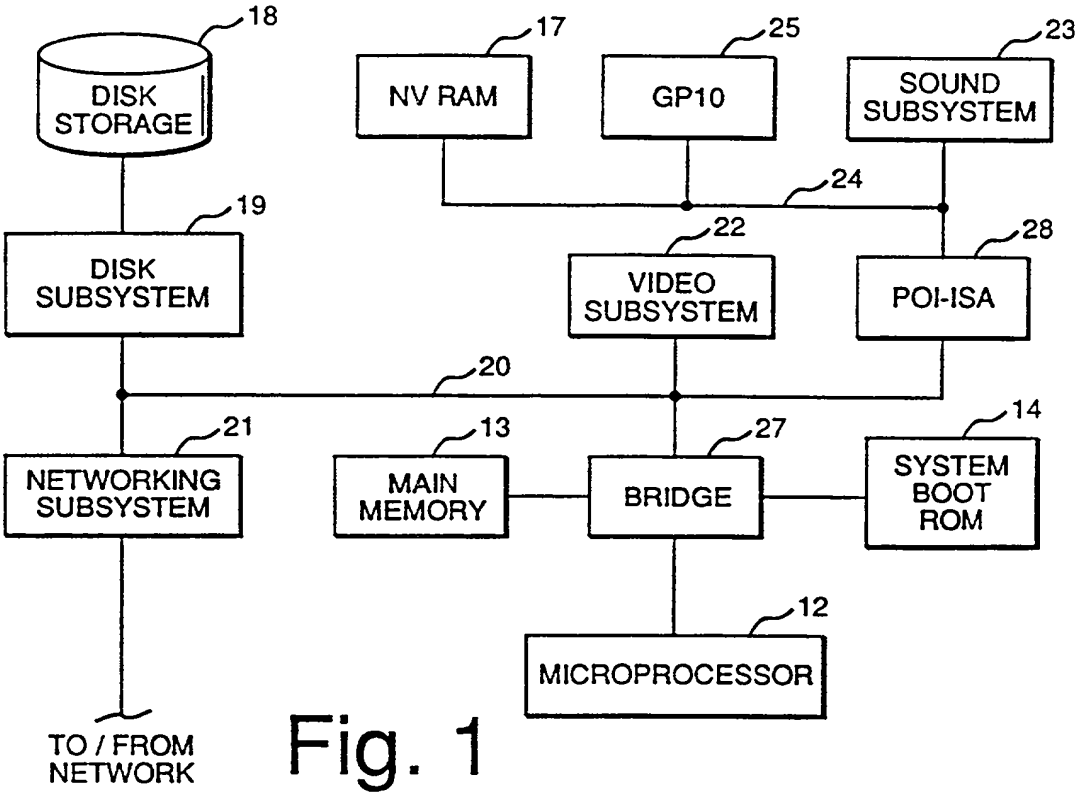

Fig. 1

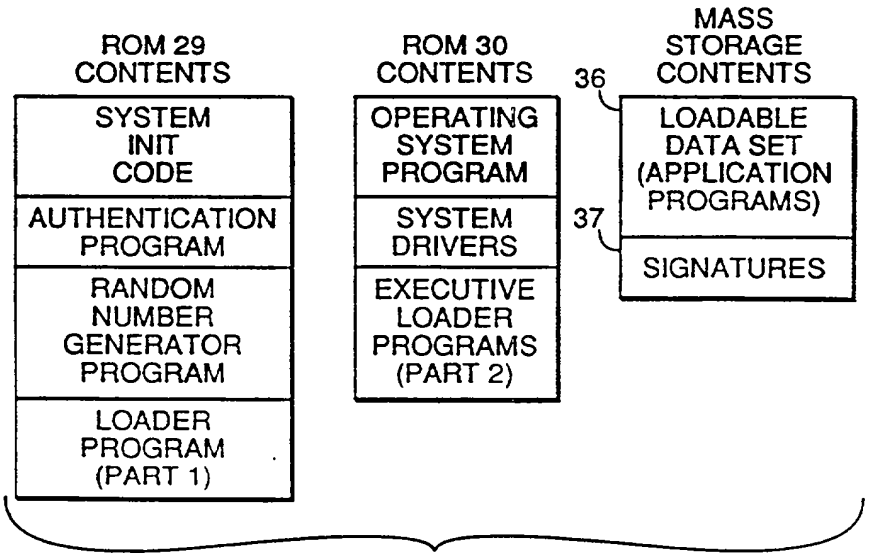

Fig. 2

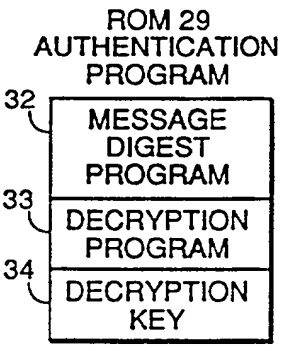

Fig. 3

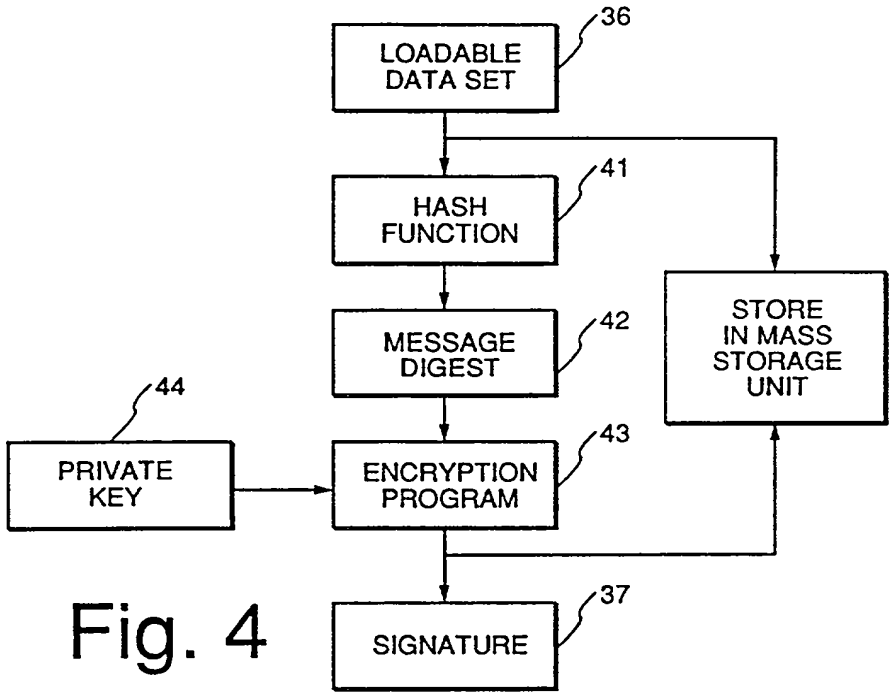
LOADABLE DATA SET
36
HASH FUNCTION
41
MESSAGE DIGEST
42
STORE IN MASS STORAGE UNIT
PRIVATE KEY
44
ENCRYPTION PROGRAM
43
SIGNATURE
37

Fig. 4

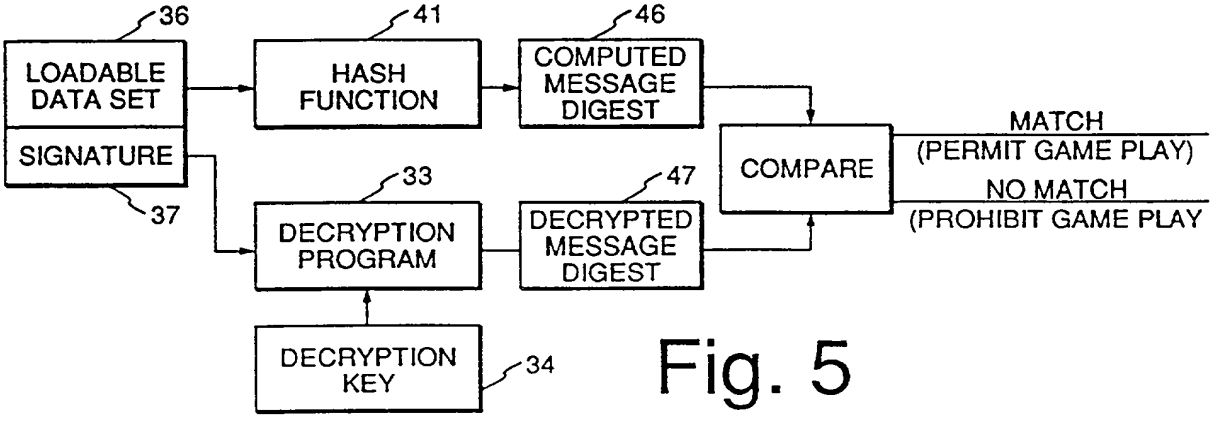
LOADABLE DATA SET
36
SIGNATURE
37
HASH FUNCTION
41
COMPUTED MESSAGE DIGEST
46
DECRYPTION PROGRAM
33
DECRYPTED MESSAGE DIGEST
47
DECRYPTION KEY
34
COMPARE
MATCH
(PERMIT GAME PLAY)
NO MATCH
(PROHIBIT GAME PLAY

Fig. 5

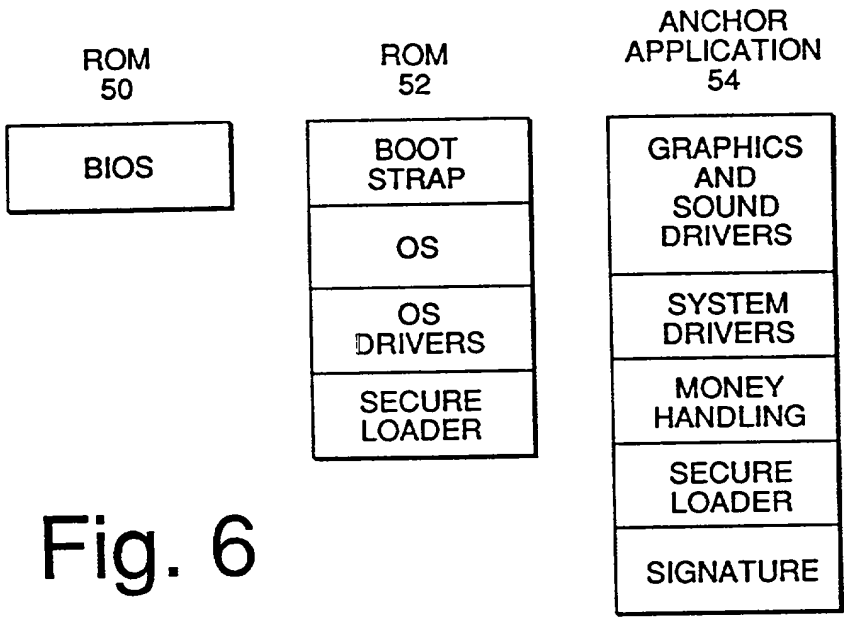
ROM
50
BIOS
ROM
52
BOOT
STRAP
OS
OS
DRIVERS
SECURE
LOADER
ANCHOR
APPLICATION
54
GRAPHICS
AND
SOUND
DRIVERS
SYSTEM
DRIVERS
MONEY
HANDLING
SECURE
LOADER
SIGNATURE

Fig. 6

#3

DECLARATION AND POWER OF ATTORNEY

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **"Electronic Casino Gaming System With Improved Play Capacity, Authentication and Security"**,

the specification of which

(check one) ___is attached hereto.
__X__was filed on December 29, 1998 as Serial Number 08/981, 882.

I hereby state that I have reviewed and understand the content of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed
PCT/US96/10463	WIPO	17 June 1996	Yes
(Number)	(Country)	(Day/Month/Year Filed)	

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

08/925,991	09/09/97	pending
(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)

Power of Attorney: I hereby appoint the following patent attorneys and/or patent agent(s) with full power of appointment, substitution and revocation to prosecute this application, to make alterations and amendments thereto, to receive the patent, and to transact all business connected therewith in the U.S. Patent and Trademark Office and in all foreign patent offices in which corresponding applications for patent are filed.

CLAUDE A.S. HAMRICK, Reg. ~~22,586~~
ROBERT O. GUILLOT, Reg. No. 28,852
EMIL C. CHANG, Reg. No. 37,593
MARYAM IMAM, Reg. No. 38,190
JUSTIN F. BOYCE, Reg. No. 40,920
LARRY E. HENNEMAN, JR., Reg, No. 41,063
CHIEN W. CHOU, Reg. No. P-41,672

Address all telephone calls to Claude A.S. Hamrick at (408) 275-8790, and address all correspondence to:

CLAUDE A.S. HAMRICK, Esq.
OPPENHEIMER POMS SMITH
10 Almaden Boulevard, Suite 600
San Jose, California 95113

- I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Full Name of Sole or First Inventor: Allan E. Alcorn

Home Address: 660 Los Trancos Road, Portola Valley, California 94028

Post Office Address: Same as above

Citizenship: United States

Inventor's Signature. Allan E Alcorn Date: 3/3/98

Full Name of Second Inventor: Michael Barnett

Home Address: 243 Buena Vista Ave, #316, Sunnyvale, CA 94086

Post Office Address: Same as above

Citizenship: United States

Inventor's Signature: Michael Barnett Date: 2/26/98

over

Full Name of Third Inventor: 3-00 Louis D. Giacalone, Jr.

Home Address: ~~922 Celia Street, Palo Alto, California 94303~~ 7450 S. Eastern Ave, #2002, Las Vegas NV 89123

Post Office Address: Same as above

Citizenship: United States

Inventor's Signature: _____ Date: 2/27/98

Full Name of Fourth Inventor: 4-00 Adam E. Levinthal

Home Address: 956 Wilmington Way, Redwood City, California 94062 CA

Post Office Address: Same as above

Citizenship: United States

Inventor's Signature: Adam Levinthal Date: 2/27/98

#3

Attorney's File No: 38184-0026US
Applicants: Allan E. Alcorn, Michael Barnett, Louis D.Giacalone, Jr. and Adam E.Levinthal
Serial Number: 08/981,882 Filed: December 29, 1998

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27(c) - SMALL BUSINESS CONCERN

I am:

- ☐ the owner of the small business concern identified below;
- ☒ an official of the small business concern empowered to act on behalf of the concern identified below;

Name of Concern: Silicon Gaming, Inc.

Address of Concern: 2800 West Bayshore Highway
Palo Alto, CA 94303

I hereby declare that the above-identified small business concern qualifies as a small business concern as defined in 13 CFR 121.318, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full time, part-time, or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled **"Electronic Casino Gaming System With Improved Play Capacity, Authentication and Security"** by Allan E. Alcorn, Michael Barnett, Louis D. Giacalone, Jr. and Adam E. Levinthal, and described in the specification described in Serial No. 08/981,882 filed on December 29, 1998.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

*NOTE: Separate Verified Statements are required from each named person, concern, or organization having rights to the invention averring to their status as small entities (37 CFR 1.27)

NAME: _____
ADDRESS: _____

( ) INDIVIDUAL ( ) SMALL BUSINESS ( ) NONPROFIT ORGANIZATION

I acknowledge my duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the

earliest of the Issue Fee or any Maintenance Fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful, false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Verified Statement is directed.

Name of Person Signing:	Jeffrey Friedberg
Title:	Vice President, Engineering
Address of Person Signing:	Silicon Gaming, Inc. 2800 West Bayshore Highway Palo Alto, CA 94303

Signature  Date: 2/26/98